

UNITED STATES DISTRICT COURT

for the
Eastern District of Virginia

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)

16 Cedarview Court, Fredericksburg, Virginia 22406

Case No.

3:17SW161

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

16 Cedarview Court, Fredericksburg, Virginia 22406

located in the Eastern District of Virginia, there is now concealed (identify the person or describe the property to be seized):

Items listed in Attachment B to affidavit in support of this application, incorporated herein,

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☒ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. Section 1028A	Aggravated identity theft
18 U.S.C. Section 1542	False statements etc. on passport application

The application is based on these facts:
Attached affidavit

- ☒ Continued on the attached sheet.
- ☒ Delayed notice of days (give exact ending date if more than 30 days:) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Reviewed by AUSA/SAUSA:

S. David Schiller

Applicant's signature

Printed name and title

Sworn to before me and signed in my presence.

Date: August 9, 2017

City and state: Richmond, Virginia

IS/
David J. Novak
United States Magistrate Judge

Judge's signature

Printed name and title

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA
Richmond Division

IN THE MATTER OF THE SEARCH OF:)	
)	CASE NO.
16 Cedarview Court, Fredericksburg, Virginia,)	
22406)	
)	UNDER SEAL

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH AND SEIZURE WARRANT**

I, Christopher Holmes, being first duly sworn, hereby depose and state as follows:

BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as 16 Cedarview Court, Fredericksburg, Virginia, 22406, hereinafter "SUBJECT PREMISES," further described in Attachment A, for the things described in Attachment B.

2. I am a Special Agent with the Diplomatic Security Service, United States Department of State ("DSS"), and have been since September 19, 2016. I am presently assigned to the Washington Field Office as a criminal investigator. As a federal agent, I am authorized to investigate violations of laws of the United States, and as a law enforcement officer I am authorized to execute warrants issued under the authority of the United States.

3. I have received training in law enforcement and criminal law from both the Federal Law Enforcement Training Center in Glynco, Georgia and the U.S. Department of State Diplomatic Security Service Basic Special Agent Course. I have participated in and conducted numerous investigations into various types of criminal violations, including travel document and

immigration fraud.

4. This affidavit is based upon information that I have obtained from my personal observations, witness interviews, my training and experience, review of documentary evidence, and information provided to me by other members of the investigation. Because this affidavit is submitted only for the limited purpose of establishing probable cause for a search warrant, it does not include all information known to the government as a result of the investigation.

5. Based on my training and experience and the facts as set forth in this affidavit, I submit that there is probable cause to believe that **MARBIN JEOVANY DIAZ** is using, and has used, the SUBJECT PREMISES to commit and facilitate the commission of violations of aggravated identity theft, in violation of Title 18, United States Code, Section 1028A and making false statements in a passport application, in violation of Title 18, United States Code, Section 1542. In addition, I submit that there is probable cause to believe that the SUBJECT PREMISES contain documents, records, financial records, correspondence, and other materials that constitute evidence, fruits and instrumentalities of the aforementioned crimes, and disposition of the proceeds from the crimes under investigation. I submit that there is also probable cause to search the information described in Attachment A for evidence of these crimes further described in Attachment B.

PROBABLE CAUSE

6. On February 23, 2017, the defendant purporting to be **FRANCISCO JAVIER VALDES REYES** applied for a U.S. passport at the US Post Office in Sealston, VA, in the Eastern District of Virginia, providing a Puerto Rican birth certificate and a Virginia State driver's license as proof of identity. The applicant swore to the veracity of, and signed the

application, authorizing the United States Department of State to issue a U.S. Passport in the name of **FRANCISCO JAVIER VALDES REYES**.

7. A Facebook profile for “Chico Diaz” was linked to the phone number “540-455-5326” which was listed by SUBJECT in Field 7 on the passport application (DS-11). The photographs in the “Chico Diaz” Facebook profile strongly resembled SUBJECT’s photograph submitted with the DS-11. The Facebook profile indicated that “Chico Diaz” has a daughter named “Diana Diaz Canas” whose mother is named “Yancy Canas”.

8. The U.S. Department of State’s Consular Consolidated Databases shows two U.S. passports issued in the name Diaz Canas, Diana Patricia with a date of birth of January 11, 2008: U.S. Passport No. 441549697 was issued January 11, 2008 and U.S. Passport No. 558842101 was issued March 15, 2017. On both of Diaz Canas’s passport applications from 2008 and 2017, the applicant listed her father’s name as “**MARBIN JEOVANY DIAZ**”. The 2017 passport application for Diaz Canas was executed on February 27, 2017 at the Falmouth Branch Post Office in Fredericksburg, VA, and the acceptance agent made copies of the parents’ passports offered as proof of the parents’ identities. The father’s passport was Honduran Passport No. #E627966 in the name of **DIAZ DIAZ, MARBIN JEOVANY**, issued on September 9, 2013 and due to expire on September 9, 2023. The photograph in the Honduran passport for **DIAZ DIAZ, MARBIN JEOVANY** resembled the individual that applied for a U.S. Passport in Sealston, VA, on February 23, 2017 as **FRANCISCO JAVIER VALDES REYES**.

9. On March 30, 2017, a search of the U.S. Department of State’s Consular Lookout and Support System (CLASS) indicated that **MARBIN JEOVANY DIAZ** (POB: Honduras, DOB: 04 OCT 1986) may be wanted by ICE for potential deportation (A#098619516, UID:

ICEAB098619516, TECS ID-P5516072400B06). A search of U.S. Citizenship and Immigration Services (USCIS) for the name **MARBIN JEOVANY DIAZ** returned results stating the individual was arrested in Stafford County, Virginia in 2007 and was subject to an ICE detainer on September 13, 2007 as **MARBIN JEOVANY DIAZ** had no valid immigration status in the United States at the time of his arrest. In addition, the system showed convictions in September 2007 for Possession of a Fictitious ID, Failure to Appear to Arraignment, and Driving on a Suspended License.

10. On April 19, 2017, the San Juan Regional Office for Diplomatic Security provided the investigating agent with a Puerto Rican Driver's License photograph and a booking photograph of an individual believed to be the "true" Francisco Javier Valdes Reyes. The photograph of Valdes Reyes from Puerto Rico is not consistent with the photograph of the **FRANCISCO JAVIER VALDES REYES** that submitted with the DS-11 executed in Sealston, VA on February 23, 2017.

11. On May 10, 2017, Special Agents from the Diplomatic Security San Juan Regional Office Task Force in Puerto Rico interviewed Francisco Javier Valdes Reyes and his mother at their home located at Barrio Vega Redonda, PR-172, KM4.1, Comerio, PR. The agents obtained a photograph of Valdes Reyes, his mother, Puerto Rican Driver's License, Voter Registration Card, and identifying tattoos. Valdes Reyes and his mother, Maribel Reyes Rios, attested in separate voluntary statements that Valdes Reyes had never been to Virginia and never applied for a U.S. Passport before. Additionally, neither Valdes Reyes nor Maribel Reyes Rios recognized a photograph of the **FRANCISCO JAVIER VALDES REYES** that submitted with the DS-11 executed in Sealston, VA on February 23, 2017.

12. **MARBIN JEOVANY DIAZ** has violated Title 18, United States Code, Sections 1542 (False statement in a passport application) and Title 18 United States Code 1028A (Aggravated identity theft) in that he made false statements in an application for a United States Passport by representing himself to be **FRANCISCO JAVIER VALDES REYES** an American citizen, knowing said statements to be false, and that he willfully and knowingly used a means of identification of another person to aid the unlawful activity with the intent to secure the issuance of a passport and the rules prescribed pursuant to such laws under the authority of the United States.

SUBJECT PREMISES

13. My investigation has revealed that **MARBIN JEOVANY DIAZ** lives at the SUBJECT PREMISES with Yancy Canas, a daughter; Diana Patricia Diaz Canas; and possibly a teenage son. I have observed five vehicles in the parking lot and driveway to SUBJECT PREMISES. Two of these vehicles, a silver 2006 Toyota Sienna with Virginia license plate number VWA7492 and a black 2007 Toyota Yaris with Virginia license plate number ZR1787, are registered to Yancy Canas, the mother of **MARBIN JEOVANY DIAZ**'s daughter Diana Patricia Diaz Canas. Both vehicles were observed by Special Agent Holmes on May 8, May 17, July 7, and July 11, 2017 parked in the driveway of the SUBJECT PREMISES.

14. The SUBJECT PREMISES was also listed as the mailing address on Diana Patricia Diaz Canas's passport application for U.S. Passport No. 558842101, issued March 15, 2017. The SUBJECT PREMISES was listed on a gym membership application listing SUBJECT as an applicant to "Anytime Fitness" at 27 S. Gateway Dr. Suite 115, Fredericksburg VA, 22405 executed December 21, 2015. Anytime Fitness entry badging records indicate that a

FRANCISCO VALDES REYES regularly attends the Anytime Fitness location where the contract was executed.

15. On July 11, 2017 at approximately 0118HRS local time, I observed a black 2007 Toyota Yaris with Virginia license plate ZR1787 park in front of Anytime Fitness at 27 S. Gateway Dr. Suite 115, Fredericksburg VA, 22405. I observed **MARBIN JEOVANY DIAZ** exit the driver seat and a young teenage male exit the passenger seat. Both males opened the door to the Anytime Fitness at the aforementioned location and entered the facility. I observed both males conducting physical activity in the gym before exiting the location at approximately 0218HRS local time. Additionally, I observed a black Toyota Yaris enter the SUBJECT PREMISES neighborhood at the intersection of Village Parkway and Shadowbrook Lane at approximately 0227HRS local time. I physically observed that a black Toyota Yaris with Virginia license plate ZR1787 was parked in the driveway of the SUBJECT PREMISES.

16. Based on my training and experience people park their vehicles at their residence or domicile, particularly during evening and early morning hours. The frequency which the vehicles registered to Yancy Canas, the mother of **MARBIN JEOVANY DIAZ**'s child, are parked in the driveway of the SUBJECT PREMISES suggests the owner and operators of said vehicles resides at SUBJECT PREMISES. My observation of **MARBIN JEOVANY DIAZ** operating a black 2007 Toyota Yaris with Virginia license plate ZR1787 registered to Yancy Canas indicates that **MARBIN JEOVANY DIAZ** is an authorized operator of said vehicle and resides at SUBJECT PREMISES.

17. Based on my training and experience, individuals that commit aggravated identity theft in violation of Title 18, United States Code, Section 1028A and passport fraud in violation

of Title 18, United States Code, Section 1542 commonly keep the fruits and instrumentalities of criminal activity at their residence.

TECHNICAL TERMS

18. Based on my training and experience, and information acquired from other law enforcement officials with technical expertise, I know the terms described below have the following meanings or characteristics:

a. “Computer” means “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.” See 18 U.S.C. § 1030(e)(1).

b. “Computer hardware” means all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, modems, routers, scanners and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

c. “Computer passwords and data security devices” means information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a

string of alpha-numeric characters) usually operates a digital key to “unlock” particular data security devices.

d. IP Address: The Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

e. The Internet is a global network of computers and other electronic devices that communicate with each other using numerous specified protocols. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

f. “Website” consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

g. “Cache” means the text, image, and graphic files sent to and temporarily stored by a user’s computer from a website accessed by the user in order to allow the user speedier access to and interaction with that website.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

19. As described above and in Attachment B, this application seeks permission to search for records that might be found on the SUBJECT PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or on other electronic storage media or digital devices. As used herein, the terms "electronic storage media" and "digital devices" include any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop computers, laptop computers, notebooks, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, USB flash drives, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices. Thus, the warrant applied for would authorize the seizure of electronic storage media and digital devices or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

20. *Probable Cause.* Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I respectfully submit that if electronic storage media or digital devices are found on the SUBJECT PREMISES, there is probable cause to believe that the records and information described in Attachment B will be stored in the electronic storage media and digital devices for at least the following reasons:

- a. Individuals who engage in passport fraud often use electronic devices, including, but not limited to, smart phones and computers to receive or transmit personal identification data for use in identity theft.
- b. Individuals who engage in the foregoing criminal activity, in the event that they change computers, will often “back up” or transfer files from their old computers’ hard drives to that of their new computers, so as not to lose data, including that described in the foregoing paragraph, which would be valuable in facilitating their criminal activity.
- c. Computer, smart phone, and other digital device files, or remnants of such files, can be recovered months or even years after they have been downloaded onto an electronic storage medium, deleted, or viewed via the Internet. Electronic files downloaded to an electronic storage medium can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools. When a person “deletes” a file on a digital device such as a home computer or a smart phone, the data contained in the file does not actually disappear; rather, that data remains on the electronic storage medium until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the electronic storage medium that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space – for long periods of time before they are overwritten. In addition, a digital device’s operating system may also keep a record of deleted data in a “swap” or

“recovery” file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or “cache.” The browser typically maintains a fixed amount of electronic storage medium space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve “residue” of an electronic file from an electronic storage medium depends less on when the file was downloaded or viewed than on a particular user’s operating system, storage capacity, and computer, smart phone, or other digital device habits.

21. *Forensic Evidence.* As further described in Attachment B, this application seeks permission to locate not only electronic evidence or information that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence or information that establishes how electronic storage media or digital devices were used, the purpose of their use, who used them, and when. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I respectfully submit there is probable cause to believe that this forensic electronic evidence and information will be on electronic storage media and digital devices in the SUBJECT PREMISES because:

- a. Although some of the records called for by this warrant might be found in the form of user-generated documents or records (such as word processing, picture, movie, or texting files), digital devices can contain other forms of electronic evidence as well. In particular, records of how a digital device has been used, what it has been used for, who has used it, and who has been responsible for

creating or maintaining records, documents, programs, applications, and materials contained on the digital devices are, as described further in the attachments, called for by this warrant. Those records will not always be found in digital data that is neatly segregatable from the hard drive, flash drive, memory card, or other electronic storage media image as a whole. Digital data on the electronic storage media not currently associated with any file can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on a hard drive that show what tasks and processes on a computer were recently used. Web browsers, e-mail programs, and chat programs often store configuration data on a hard drive, flash drive, memory card, or memory chip that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and the times a computer, smart phone, or other digital device was in use. Computer, smart phone, and other digital device file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations. Recovery of this data requires specialized tools and a controlled laboratory environment, and also can require substantial time.

- b. Forensic evidence on a computer or storage medium can also indicate who has used or controlled the computer or storage medium. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, “chat,” instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time.
- c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, electronic storage media and digital device evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on electronic storage media or digital devices is evidence may depend on other information stored on the devices and the application of knowledge about how the devices behave. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

- e. Further, in finding evidence of how electronic storage media or a digital device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on the device. For example, the presence or absence of counter-forensic programs, anti-virus programs (and associated data), and malware may be relevant to establishing the user's intent and the identity of the user.

22. *Methods To Be Used To Search Digital Devices.* Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I know that:

- a. Searching digital devices can be an extremely technical process, often requiring specific expertise, specialized equipment, and substantial amounts of time. There are so many types of digital devices and software programs in use today that it is impossible to bring to the search site all of the necessary technical manuals, specialized equipment, and software programs necessary to conduct a thorough search. Digital devices – whether, for example, desktop computers, mobile devices, or portable storage devices – may be customized with a vast array of software applications, each generating a particular form of information or records and each often requiring unique forensic tools, techniques, and expertise. As a result, it may be necessary to consult with specially trained personnel who have specific expertise in the types of digital devices, operating systems, or software applications that are being searched, and to obtain specialized hardware and software solutions to meet the needs of a particular forensic analysis.

- b. Digital data is particularly vulnerable to inadvertent or intentional modification or destruction. Searching digital devices can require the use of precise, scientific procedures that are designed to maintain the integrity of digital data and to recover “hidden,” erased, compressed, encrypted, or password-protected data. Recovery of “residue” of electronic files from electronic storage media also requires specialized tools and often substantial time. As a result, a controlled environment, such as a law enforcement laboratory or similar facility, is essential to conducting a complete and accurate analysis of data stored on digital devices.
- c. The volume of data stored on many digital devices will typically be so large that it will be extremely impractical to search for data during the physical search of the premises. Smart phones capable of storing 64 gigabytes, flash drives capable of storing 128 gigabytes, and desktop computers capable of storing 500 or more gigabytes are now commonplace. Consequently, just one device might contain enormous amounts of data.
- d. Further, as discussed above, evidence of how a digital device has been used, the purposes for which it has been used, and who has used it, may be reflected in the absence of particular data on a digital device. For example, to rebut a claim that the owner of a digital device was not responsible for a particular use because the device was being controlled remotely by malicious software, it may be necessary to show that malicious software that allows someone else to control the digital device remotely is not present on the digital device. Evidence of the absence of particular data or software on a digital device is not segregatable from the digital

device itself. Analysis of the digital device as a whole to demonstrate the absence of particular data or software requires specialized tools and a controlled laboratory environment, and can require substantial time.

- e. Digital device users can attempt to conceal data within digital devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension “.jpg” often are image files; however, a user can easily change the extension to “.txt” to conceal the image and make it appear that the file contains text. Digital device users can also attempt to conceal data by using encryption, which means that a password or device, such as a “dongle” or “keycard,” is necessary to decrypt the data into readable form. Digital device users may encode communications or files, including substituting innocuous terms for incriminating terms or deliberately misspelling words, thereby thwarting “keyword” search techniques and necessitating continuous modification of keyword terms. Moreover, certain file formats, like portable document format (“PDF”), do not lend themselves to keyword searches. Some applications for computers, smart phones, and other digital devices, do not store data as searchable text; rather, the data is saved in a proprietary non-text format. Documents printed by a computer, even if the document was never saved to the hard drive, are recoverable by forensic examiners but not discoverable by keyword searches because the printed document is stored by the computer as a graphic image and not as text. In addition, digital device users can conceal data within another seemingly unrelated and innocuous file in a process called

“steganography.” For example, by using steganography a digital device user can conceal text in an image file that cannot be viewed when the image file is opened. Digital devices may also contain “booby traps” that destroy or alter data if certain procedures are not scrupulously followed. A substantial amount of time is necessary to extract and sort through data that is concealed, encrypted, or subject to booby traps, to determine whether it is evidence, contraband or instrumentalities of a crime.

- f. Analyzing the contents of mobile devices can be very labor intensive and also requires special technical skills, equipment, and software. The large, and ever increasing, number and variety of available mobile device applications generate unique forms of data, in different formats, and user information, all of which present formidable and sometimes novel forensic challenges to investigators that cannot be anticipated before examination of the device. Additionally, most smart phones and other mobile devices require passwords for access. For example, even older iPhone 4 models, running IOS 7, deployed a type of sophisticated encryption known as “AES-256 encryption” to secure and encrypt the operating system and application data, which could only be bypassed with a numeric passcode. Newer cell phones employ equally sophisticated encryption along with alpha-numeric passcodes, rendering most smart phones inaccessible without highly sophisticated forensic tools and techniques, or assistance from the phone manufacturer. Mobile devices used by individuals engaged in criminal activity are often further protected and encrypted by one or more third party applications,

of which there are many. For example, one such mobile application, "Hide It Pro," disguises itself as an audio application, allows users to hide pictures and documents, and offers the same sophisticated AES-256 encryption for all data stored within the database in the mobile device.

- g. Based on all of the foregoing, I respectfully submit that searching any electronic storage media or digital device for the information, records, or evidence subject to seizure pursuant to this warrant may require a wide array of electronic data analysis techniques and may take weeks or months to complete. Any pre-defined search protocol would only inevitably result in over- or under-inclusive searches, and misdirected time and effort, as forensic examiners encounter technological and user-created challenges, content, and software applications that cannot be anticipated in advance of the forensic examination of the media or devices. In light of these difficulties, your affiant requests permission to use whatever data analysis techniques reasonably appear to be necessary to locate and retrieve digital information, records, or evidence within the scope of this warrant.
- h. In searching for information, records, or evidence, further described in Attachment B, law enforcement personnel executing this search warrant will employ the following procedures:
 - 1. Upon securing the SUBJECT PREMISES, law enforcement personnel will, consistent with Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure, seize any electronic storage media or digital devices, as defined above, deemed capable of containing the

information, records, or evidence described in Attachment B and transport these items to an appropriate law enforcement laboratory or similar facility for review. For all the reasons described above, it would not be feasible to conduct a complete, safe, and appropriate search of any such electronic storage media or digital devices at the PREMISES. The electronic storage media and digital devices, and/or any digital images thereof created by law enforcement in aid of the examination and review, will be examined and reviewed by law enforcement personnel in order to extract and seize the information, records, or evidence described in Attachment B.

2. The analysis of the contents of any seized electronic storage media or digital devices may entail any or all of various forensic techniques as circumstances warrant. Such techniques may include, but shall not be limited to, surveying various file “directories” and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files); conducting a file-by-file review by “opening,” reviewing, or reading the images or first few “pages” of such files in order to determine their precise contents; “scanning” storage areas to discover and possibly recover recently deleted data; scanning

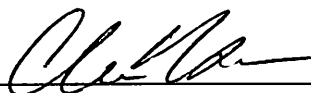
storage areas for deliberately hidden files; and performing electronic “keyword” searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are related to the subject matter of the investigation.

3. In searching the seized electronic storage media or digital devices, the forensic examiners may examine as much of the contents of the electronic storage media or digital devices as deemed necessary to make a determination as to whether the contents fall within the items to be seized as set forth in Attachment B. In addition, the forensic examiners may search for and attempt to recover “deleted,” “hidden,” or encrypted data to determine whether the contents fall within the items to be seized as described in Attachment B. Any search techniques or protocols used in searching the contents of the seized electronic storage media or digital devices will be specifically chosen to identify only the specific items to be seized under this warrant.

CONCLUSION

23. Based on the foregoing, I have probable cause to believe that within the SUBJECT PREMISES, as further described in Attachment A, and incorporated herein by reference, there is evidence of violations of Title 18, United States Code, Sections 1028A, and 1542, and that the items listed in Attachment B, constituting evidence, fruits or instrumentalities of those violations, will be located therein. I therefore respectfully request that the Court issue a warrant authorizing me and other law enforcement officers to search the SUBJECT PREMISES described in Attachment A, and to seize the items listed in Attachment B.

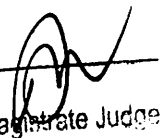
Respectfully submitted,



Christopher R. Holmes, Special Agent
Diplomatic Security Service
United States Department of State

Subscribed and sworn to before me
on August 9, 2017:

/s/



David J. Novak
United States Magistrate Judge

UNITED STATES MAGISTRATE JUDGE

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Richmond Division

IN THE MATTER OF THE SEARCH OF:)

16 Cedarview Court, Fredericksburg, Virginia,)
22406)

CASE NO. 3:17SW161

UNDER SEAL

ATTACHMENT A

Property to be searched

The property to be searched is 16 Cedarview Court, Fredericksburg, Virginia, 22406 (the "SUBJECT PREMISES"). The SUBJECT PREMISES is a two-story, detached single-family home. The SUBJECT PREMISES sits at the end of a driveway stemming from the south side of Cedarview Court. The SUBJECT PREMISES is taupe in color, with a light brown roof. The SUBJECT PREMISES has east-facing red front door and two car garage.



IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Richmond Division

IN THE MATTER OF THE SEARCH OF:)

16 Cedarview Court, Fredericksburg, Virginia,)
22406)

CASE NO. 3:17sw161

UNDER SEAL

ATTACHMENT B

Property to be seized

1. The items to be seized are MARBIN JEOVANY DIAZ, fruits, evidence, records and information relating to, contraband, or instrumentalities of violations of aggravated identity theft, in violation of Title 18, United States Code, Section 1028A, making false statements in a passport application, in violation of Title 18, United States Code, Section 1542, in the Eastern District of Virginia, in Attachment A:

- a. The person MARBIN JEOVANY DIAZ;
- b. All records, documents and communications or other information related to the citizenship, residency, and immigration status of MARBIN JEOVANY DIAZ including passports, applications for status with the Department of Homeland Security and subsidiary entities, driver's licenses, birth certificates, and social security cards;
- c. All citizenship documents and residency status documents relating to FRANCISCO JAVIER VALDES REYES, including driver's licenses, birth certificates, and social security cards;

- d. All financial records relating to FRANCISCO JAVIER VALDES REYES or MARBIN JEOVANY DIAZ including banking statements, financial transaction receipts, voided checks, or financial applications;
- e. All financial instrumentalities that contain identification information such as credit cards, debit cards, and checks bearing the names of MARBIN JEOVANY DIAZ, MARVIN JEOVANY DIAZ, MARBIN HERWANI DIAZ, FRANCISCO JAVIER VALDES REYES or any disambiguation of the aforementioned names;
- f. All records, documents and communications or other information related to or showing compensation given in exchange for the obtaining or exchange of United States citizen documentation such as birth certificates;
- g. Passports both foreign and domestic, visas, tickets, photographs, and other evidence related to international travel, residency, or birth in a foreign country;
- h. All records requesting new or updated birth certificates from any government or private entity;
- i. Any records, documents and communications, handbooks, instructions or other documents showing knowledge, instructions or guidance regarding the U.S. immigration laws, applications or process for seeking immigration benefits;
- j. All records, documents and communications or other information showing payments, including logs or records by, to or from others with regards to immigration benefits sought or obtained;
- k. U.S. or foreign currency;
- l. Any item clearly identifiable as contraband.

2. For any electronic storage media or digital device whose seizure is otherwise authorized by this warrant, and any electronic storage media or digital device that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, “COMPUTER”):

- a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence;
- b. evidence of software, or the lack thereof, that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- d. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- e. evidence of the times the COMPUTER was used;
- f. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- g. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

- h. records of or information about Internet Protocol addresses used by the
COMPUTER;
- i. records of or information about the COMPUTER's Internet activity, including
firewall logs, caches, browser history and cookies, "bookmarked" or "favorite"
web pages, search terms that the user entered into any Internet search engine, and
records of user-typed web addresses.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The terms "electronic storage media" and "digital devices" include any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop computers, laptop computers, notebooks, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, USB flash drives, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); security devices; and any other type of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions.